REMARKS/ARGUMENT

1) Claims 1, 4-7 and 10-12 stand rejected under 35 U.S.C. 102(e) as being anticipated by Gray, US patent, 6,268,788. Applicants respectfully traverse this rejection as set forth:

Independent Claim 1, as amended, requires and positively recites, a method of securing access to resources in a computing device, comprising the steps of: "storing an encrypted access code **in a memory location within the computing device**", "receiving a password to access the resources", "encrypting the password to produce a encrypted password", "comparing the encrypted password to the encrypted access code", and "allowing access to the resources if the encrypted access code matches the encrypted password".

Independent Claim 7, as amended, requires and positively recites, a computing device comprising: "a processing system", "a **memory coupled to the processing system for storing an encrypted access code**", "input circuitry coupled to the processing system for receiving a password to access resources, wherein the processing circuitry: encrypts the password to produce a encrypted password; compares the encrypted password to the encrypted access code; and allows access to the resources if the encrypted access code matches the encrypted password".

In contrast, Gray clearly shows that verification unit 20 is not part of computer 12. Verification unit 20 is externally interposed between keyboard 16 and computer 12 (see Figs. 1, 2; col. 4, lines 13-20). Further, to the extent verification unit 20 has memory, it is not used to store any access code (much less an encrypted access code) for obtaining access to computer 12. Indeed, Gray teaches that verification data such as a security

identification number, a password, or a Personal Identification Number (PIN) of the operation requesting control of the application software is stored on card 34 (col. 4, lines 31-38) – NOT within memory within computer 12 or memory within verification unit 20. Moreover, it is the card 34 that issues a "pass" or a "fail" signal via verification unit 20 to the computer 12, which either grants or denies execution control of application software to the operation (col. 4, lines 39-42). Accordingly, Gray fails to teach or suggest, "storing an encrypted access code **in a memory location within the computing device**", as required by Claim 1, OR a computing device comprising: "a processing system" and "a **memory coupled to the processing system for storing an encrypted access code**", as required by Claim 7.

In light of the above, it should be clear that that each and every element of Claims 1 and 7 are NOT found expressly, or inherently, in the Gray reference. See, *Verdegall Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See also, *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)". Accordingly, the 35 U.S.C. 102(e) rejection of Claims 1 and 7 is overcome.

Claims 4-6 stand allowable as depending directly from allowable Claim 1 and Claims 10-12 stand allowable as depending directly from allowable Claim 7 and by including further limitations not taught or suggested by the reference of record.

Claim 4 further defines the method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified. Claim 4 depends from Claim 1 and is therefore allowable for the same reasons set forth above for the allowance of Claim 1.

Claim 5 further defines the method of claim 1 wherein the step of allowing access comprises the step of allowing access to testing resources if the encrypted access code matches the encrypted password. Claim 5 depends from Claim 1 and is therefore allowable for the same reasons set forth above for the allowance of Claim 1.

Claim 6 further defines the method of claim 1 wherein the step of allowing access comprises the step of allowing access to change system parameters if the encrypted access code matches the encrypted password. Claim 6 depends from Claim 1 and is therefore allowable for the same reasons set forth above for the allowance of Claim 6.

Claim 10 further defines the computing device of claim 7 wherein the encrypted access code is stored in a memory that cannot be externally modified. Claim 10 depends from Claim 7 and is therefore allowable for the same reasons set forth above for the allowance of Claim 7.

Claim 11 further defines the computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the encrypted password. Claim 11 depends from Claim 7 and is therefore allowable for the same reasons set forth above for the allowance of Claim 7.

Claim 12 further defines the computing device of claim 7 wherein the processing system allows access to system parameters if the encrypted access code matches the encrypted password. Claim 12 depends from Claim 7 and is therefore allowable for the same reasons set forth above for the allowance of Claim 7.

2) Claims 2, 3, 8 and 9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gray and Lohstroh et al, US patent 5,768,373. Applicants respectfully traverse this rejection as set forth below.

Independent Claim 1, from which Claims 2 and 3 depend directly or indirectly, requires and positively recites, a method of securing access to resources in a computing device, comprising the steps of: "storing an encrypted access code **in a memory location within the computing device**", "receiving a password to access the resources", "encrypting the password to produce a encrypted password", "comparing the encrypted password to the encrypted access code", and "allowing access to the resources if the encrypted access code matches the encrypted password".

Independent Claim 7, from which Claims 8 and 9 depend directly or indirectly, requires and positively recites, a computing device comprising: "a processing system", "a **memory coupled to the processing system for storing an encrypted access code**", "input circuitry coupled to the processing system for receiving a password to access resources, wherein the processing circuitry: encrypts the password to produce a encrypted password; compares the encrypted password to the encrypted access code; and allows access to the resources if the encrypted access code matches the encrypted password".

Claim 2 further defines the method of claim 1 wherein the step of storing an encrypted access code comprises the step of storing a hashed access code.

Claim 3 further defines the method of claim 2 wherein the step of encrypting a password comprises the step of hashing a password.

Claim 8 further defines the computing device of claim 7 wherein the encrypted access code comprises a hashed access code.

Claim 9 further defines the computing device of claim 8 wherein the encrypted password comprises a hashed password.

In contrast, Gray clearly shows that verification unit 20 is not part of computer 12. Verification unit 20 is externally interposed between keyboard 16 and computer 12 (see Figs. 1, 2; col. 4, lines 13-20). Further, to the extent verification unit 20 has memory, it is not used to store any access code (much less an encrypted access code) for obtaining access to computer 12. Indeed, Gray teaches that verification data such as a security identification number, a password, or a Personal Identification Number (PIN) of the operation requesting control of the application software is stored on card 34 (col. 4, lines 31-38) – NOT within memory within computer 12 or memory within verification unit 20. Moreover, it is the card 34 that issues a "pass" or a "fail" signal via verification unit 20 to the computer 12, which either grants or denies execution control of application software to the operation (col. 4, lines 39-42). Accordingly, Gray fails to teach or suggest, "storing an encrypted access code **in a memory location within the computing device**", as required by Claim 1, OR a computing device comprising: "a processing system" and "a **memory coupled to the processing system for storing an encrypted access code**", as required by Claim 7.

Irregardless of whether or not Lohstroh discloses the step of storing an encrypted access code comprising the step of storing a hashed access code, as recited in Claims 2, 3, 8 and 9, as argued by Examiner, Lohstroh similarly fails to teach or suggest the above-identified deficiencies of the Gray reference. Accordingly, any combination of Gray and Lohstroh fails to teach or suggest, "storing an encrypted access code **in a memory**

location within the computing device", as required by Claim 1, OR a computing device comprising: "a processing system" and "a **memory coupled to the processing system for storing an encrypted access code**", as required by Claim 7.

In proceedings before the Patent and Trademark Office, "the Examiner bears the burden of establishing a prima facie case of obviousness based upon the prior art". *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992) (citing *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984). "The Examiner can satisfy this burden **only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references**", *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992)(citing *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988)(citing *In re Lalu*, 747 F.2d 703, 705, 223 USPQ 1257, 1258 (Fed. Cir. 1988)).

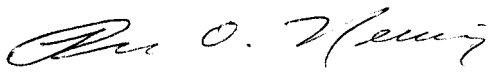
Although couched in terms of combining teachings found in the prior art, the same inquiry must be carried out in the context of a purported obvious "modification" of the prior art. **The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification.** *In re Gordon*, 733 F.2d at 902, 221 USPQ at 1127. Moreover, **it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious.** *In re Gorman*, 933 F.2d 982, 987, 18 USPQ2d 1885, 1888 (Fed.Cir.1991). See also *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1138, 227 USPQ 543, 547 (Fed.Cir.1985).

Furthermore, "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. As discussed above, Examiner has failed to set forth any legitimate suggestion or motivation, either in the references themselves or in the knowledge generally available to one or ordinary skill in that art, to combine and modify Gray and Lohstroh, as suggested by Examiner. Second, there must be a reasonable expectation of success. Examiner has failed to provide any evidence that combining Gray with Lohstroh will result in an apparatus that would successfully implement all of the elements of Claims 2, 3, 8 and 9. Finally, the prior art reference (or references when combined) must teach or suggest ALL the claim limitations (MPEP § 2143). Applicants respectfully submit that the Examiner has failed to establish all three criteria. Accordingly, Claims 2, 3, 8, and 9 are patentable under 35 U.S.C. § 103(a) over Gray in view of Lohstroh.

Claims 1-12 stand allowable over the cited art. New claims 13-46 all depend directly or indirectly from allowable Claims 1 or 7. Applicants respectfully request allowance of the application as the earliest possible date.

Respectfully submitted,



/ Ronald O. Neerings /
Reg. No. 34,227
Attorney for Applicants

TEXAS INSTRUMENTS INCORPORATED
P.O. BOX 655474, M/S 3999
Dallas, Texas 75265
Phone: 972/917-5299
Fax: 972/917-4418